John C. Kelly, Ph.D.
Jet Propulsion Laboratory

Position Paper for HDCC
Jan. 10, 11 & 12 at NASA Ames

As the nation's lead center for the robotic exploration of space, the Jet Propulsion Laboratory (JPL) is responsible for a broad spectrum of space science missions and instruments. In carrying out work for the National Aeronautics and Space Administration (NASA), JPL has developed skills and capabilities unique to deep space exploration. NASA's only federally funded research and development center, JPL is operated by the California Institute of Technology (Caltech) through a contract with NASA. JPL blends contributions from other NASA Centers, other federal laboratories, academia, industry, and the international community into high-value space missions, developing long-range perspectives and capabilities for space exploration.

JPL's Software Assurance Research program has a history of expertise and innovation in the areas of Automated Testing, Software Safety, Software Reliability, Formal Methods and Analytical Verification, Spacecraft Fault Protection, High-Criticality Product Line Architectures, and Risk Based Profiles. The leads for center initiatives at JPL have substantial research and work experience in Software Engineering, Verification and Validation, and Quality Assurance on NASA projects in addition to a high level of educational preparation (currently all have earned Ph.D. degrees). The group is active in the high-dependability community, participating via presentations of papers, tutorials, and panels, and as program committee members and chairs, at many of the major software engineering conferences (including ICSE, ISSRE, ICRE, ISRE, & HASE). Products have included research studies, tools, pilot applications, guidebooks, refereed papers, internal reports and training. These products are effectively used to transfer advanced assurance and V&V techniques into the NASA software community. As the needs of NASA projects evolve into the 21st century, JPL has maintained an excellent core group of progressive individuals to successfully research advanced technology for use on projects to support NASA's "ring of safety".

Representative Problems:

- There is a lack of substantial understanding of what it takes to make software safe and reliable. Software Engineering is significantly behind other engineering fields in the areas of safety and reliability.
- There is a lack of baseline data and metrics to objectively judge the merits of techniques and tools to improve reliability and dependability.
- Development of safety analysis techniques that can be applied and reused for an entire product line such as interferometers or spacecraft software systems
- Automated characterization of post-launch critical software anomalies with feed forward into improved system testing
- Early lifecycle software risk assessment together with lessons learned and problem/anomaly reports to derive an "optimized/tailored" assurance, IV&V and reliability program for space and aeronautics project
- Run-time monitoring of conformity to security requirements using safety analysis techniques such as fault tree analysis
- Shortage of resources and personnel devoted to the specialized techniques associated with the assurance, verification & validation of critical software systems.
- Software engineers have to continually cope with evolving software technology, tools, and languages on projects that demand high dependability. In many cases these technologies are products of organizations with very relaxed dependability requirements. The speed of change in software engineering presents a substantial intellectual challenge in itself. Keeping a balance between rapid changes in technology and assuring a product's dependability is difficult.

Technical Approaches:

The areas listed below represent technical areas of experience that JPL has an interest in seeing researched, developed and transferred within NASA projects to facilitate high dependability space and aeronautics systems.

1. Analytical Verification of Software Architectures

   The goal of this area is to support research, tools, pilot applications, and technology transfer of analytical verification approaches to NASA projects in order to improve quality and reduce the risk associated with critical software systems. Analytical verification includes a significant set of widely researched techniques and tools based on mathematical logic and rule based algorithms. As a recent example, Dr. Gerry Gannod (Arizona State) and Dr. Robyn Lutz (JPL& Iowa State) developed scenario-based architectural analysis techniques integrated with model-checking of key architectural behaviors, and applied these results to the interferometer product line at JPL.

2. Software Safety Applications

   The goal of this area is to ensure, in the dynamic environment of software development, that there are processes, tools and techniques available to assure that software will not contribute to hazardous system states. Software FMEA/FMECAs have been successfully used on flight projects at JPL, including Galileo, Cassini, DS-2, and EOS Microwave Limb Sounder. (Software FMEA, or SFMEA, is a software failure modes and effects analysis; Software FMECA has a criticality analysis added.). The most important new developments for Software FMEA to be included are: Use for software safety analysis, Integration with Software Fault Tree Analysis and system approaches, Application to product families, early use for requirements validation, and the innovative use of software safety techniques for security applications (example; the application of integrated fault-tree analysis to ensure high integrity and availability of communications across an interplanetary network). Another software safety research effort is currently underway to quantitatively characterize those critical software anomalies that escape testing and manifest themselves during flight (e.g., on Cassini, Deep Space 1, and Mars Global Surveyor), in order to improve the development process of upcoming safety-critical systems. (Key research contact: Dr. Robyn Lutz – Software Safety, JPL & Iowa State, Dr. David Gilliam, Computer Security, JPL)

3. Software Assurance for Advanced Development Technology

   The goal of this area is to research and develop techniques, tools, and guidance to address the application of software assurance in a changing development environment. Examples of advanced technologies, which needed updated assurance technology, are Object Oriented Software Architectures, Rapid Development Methods, Intelligent Agents, Automated Code Generation, and Network Aware Application. The technologies that may help address software assurance concerns include; Modeling and Analysis of requirements for fault detection, isolation, and recovery, creation of a Security Assessment Instrument for use during software development and maintenance, and the application of formalisms to networks and computer security to maintain the integrity.

4. Assurance and Verification of Autonomy for Spacecraft Applications

   Associated with JPL's mission to build robotic spacecraft to explore the solar system is the necessary use of advanced autonomy based upon sophisticated software. This area focuses on the challenges faced when assuring and verifying the quality of this unique type of software. The capability to perform effective assurance and verification for autonomous software is necessary for NASA to fulfill its goals for the 21st century. Lightweight application of V&V techniques bring emerging techniques (e.g., test oracle automation, model checking) into practical application. Projects that employ formal design descriptions (e.g., statecharts) and/or formal models (e.g., the constraints of an AI planner) exemplify systems amenable to the incorporation of these V&V techniques in a highly automated manner. This high degree of automation is key, so that they can be applied at low cost and yield their results in a timely manner. (Key research contact: Dr. Martin Feather, Dr. Ben Smith, & Dr. Nicholas Rouquette of JPL)

5. Software Reliability Estimation, Measurement, and Engineering

    This area focuses on the development of methods and tools for assessing and controlling the reliability, fault content, and risk of exposure to residual faults of a software system throughout the development and maintenance phases of the software lifecycle. Techniques developed by investigators from JPL, the Naval Postgraduate School, and Cylant Technology to use structural measurements as fault surrogates are currently being implemented in JPL and industrial development efforts to help control software fault content. Current work includes investigating relationships between measurable characteristics of requirements and the number and type of faults in the delivered product. An important long-term goal is to devise methods for preventing the insertion of faults during development, rather than being limited to identifying faults already present in the software. To accomplish this, it will be necessary to greatly improve our understanding of how developers make errors that result in software faults. (Key research contacts: Dr. Allen Nikora of JPL, Dr. Norman Schneidewind of the Naval Postgraduate School, and Dr. John Munson of Cylant)

6. Review and Evaluation of Software Engineering Products

    The goal of this area is to provide advanced techniques on effective reviews and evaluations of software engineering products to detect flaws in designs and products. This includes advancing the state of the art of reviews and evaluations for future space and aeronautics systems. This includes newer techniques like Perspective Based Reading (PBR). (Key research contacts: Dr. Vic Basili of University of Maryland, Dr. Forrest Shull, Fraunhoffer Institute, Dr. John Kelly, JPL)

7. Strategic technical planning of V&V techniques

    The strategic technical planning of assurance, reliability and V&V techniques focuses on establishing disciplined engineering activities that provide sufficient coverage of possible failure modes. JPL recently develop a Defect Detection and Prevention (DDP) process and tool. To date, the DDP approach has been applied to technology evaluations as a means to increase the infusion rates of those advanced technologies into NASA flight missions. V&V activities can be planned in the same manner: a project's risks' severities are systematically assessed by relating fault and failure information to the project requirements; V&V activities are treated as mitigators of these same risks. The net result is the ability to balance the cost effectiveness of these V&V techniques at assuring attainment of each project's goals, and plan them accordingly. (Key research contacts: Dr. Michael Greenfield of NASA HQ, Dr. Steve Conford, Dr. Martin Feather, Tom Gindorf, Tim Larson, and Burt Sigal of NASA-JPL,)

8. The integration of Model-Based Code Generation Technology with advanced V&V

    Code generators help manage software complexity by introducing useful abstractions of software that engineers across disciplines can better analyze and review. This approach allows domain-specific verification techniques to be applied in a more natural, straightforward manner than if the verification criteria have to be interpreted in terms of properties of the software implementation. Second, code generators drive a wedge in the pattern of software errors that can be traceable to systematic translation errors (a problem with the code generation process itself) or to domain-specific subsystems (where the translation similarities with other subsystems hint at domain errors instead of translation errors). This dual approach was successfully applied in the context of the Deep Space One fault protection software and is currently being revisited and augmented with additional verification techniques and commercial model-based reasoning techniques (with Mathworks, Inc.) in the context of the Deep Impact fault protection software. (Key research contacts: Dr. Nicolas Rouquette & Dr. Martin Feather of JPL)